PEACE CORPS
INCIDENT ANALYSIS & RESPONSE

Peace Corps engaged Intekras' Professional Security Services as part of their overall Information Assurance strategy. The initial requirement to conduct an indepth analysis was part of their long term strategy to implement a full Incident Response program.

Initially, *Intekras* performed a zero-knowledge discover on Peace Corps public information exposure. This process involved network reconnaissance and the gathering of information using techniques such as Google Hacking, WHOIS Interrogation, DNS Interrogation, Job Postings, and other types of Internet queries. *Intekras* provided Peace Corps with a detailed document outlining our findings and listing them in accordance to their severity.

Following the initial discovery process, *Intekras* analyzed Peace Corps systems and security event data for intrusions, anomalous behavior, strange log patterns and other events and activities that signify the need for some level of IT security triage or incident response in accordance with industry best practices. Our findings were categorized using industry best practices and US-CERT guidance and then sorted by Peace Corps Regions. Peace Corps was provided with high-level recommendations for how to handle the events/incidents which included improved incident handling procedures, log setting changes, and security architecture recommendations.

"...Peace Corps was provided with high-level recommendations for how to handle the events/incidents which included incident handling procedures, log setting changes and security architecture recommendations..."

Intekras has provided Peace Corps with a Cyber Incident Response Analyst that will respond to suspected incidents and coordinate appropriate actions with required agency personnel. This Intekras consultant also assists Peace Corps in developing, managing, communicating, and implementing an agency-wide integrated Cyber Incident Management program.